

ГО «ГРУЗИНСЬКО-УКРАЇНСЬКИЙ ЕКСПЕРТНИЙ ЦЕНТР»

**СУЧАСНІ ЗАГРОЗИ
ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ
БЕЗПЕЦІ**

МАТЕРІАЛИ

Міжнародної науково-практичної інтернет-конференції
(*м. Одеса, 29 жовтня 2023 року*)

DOI: 10.46340/GUEC2023-10

Одеса
Фенікс
2023

Редакційна колегія:

Гардапхадзе Тамара – доктор юридичних наук, професор, ректор Нового закладу вищої освіти «Newuni» (м. Тбілісі, Грузія);

Донов Олексій – голова Департаменту експертно-аналітичної діяльності щодо взаємовідносин Грузії та України ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Полухіна Аліна (укладач) – кандидат політичних наук, засновниця ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Польовий Микола – доктор політичних наук, професор, Університет імені Коминського (м. Братислава, Словачія); засновник ГО «Грузинсько-український експертний центр» (м. Одеса, Україна);

Хаджинов Ілля – доктор економічних наук, професор, ректор Донецького національного університету імені Василя Стуса (м. Вінниця, Україна);

Хевцуріані Аміран – кандидат наук з міжнародних відносин, засновник ГО «Грузинсько-український експертний центр» (м. Одеса, Україна); професор академічної кафедри політики та міжнародних відносин Грузинського технічного університету (м. Тбілісі, Грузія);

Цокур Євген – доктор політичних наук, професор, завідувач кафедри політології Запорізького національного університету (м. Запоріжжя, Україна).

Сучасні загрози глобальній та регіональній безпеці : матер. С 89 Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) [Електронне видання] / уклад. А. Полухіна ; ГО «ГУЕЦ». – Одеса : Фенікс, 2023. – 389 с. –Укр., англ., груз. мовами.

ISBN 978-617-8395-01-8

Збірник матеріалів містить матеріали доповідей, поданих на Міжнародну науково-практичну інтернет-конференцію «Сучасні загрози глобальній та регіональній безпеці», що відбулася 29 жовтня 2023 року. Подані матеріали були розглянуті під час роботи дев'яти секцій: теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки; криза сучасної системи міжнародної безпеки; регіональна безпека в нових геополітичних концепціях; основні стратегічні напрямки кібербезпеки; кіберзахист і національна безпека: український досвід; цифрова дипломатія в умовах трансформації системи міжнародної безпеки; фейки та дідфейки як інструменти негативного впливу на національну безпеку; фактчекінг як інструмент протидії в гібридній війні; державне управління та національна безпека.

Збірник адресовано науковим, науково-педагогічним працівникам, здобувачам закладів вищої освіти, громадським організаціям, журналістам, незалежним експертам і всім, хто цікавиться проблемами загроз глобальній та регіональній безпеці.

УДК 327.7:355.02

© ГО «Грузинсько-український експертний центр», 2023

ISBN 978-617-8395-01-8

© Колектив авторів, 2023

З М І С Т

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

Чальцева О. М. Новий світопорядок в умовах конфліктного середовища	9
Davit Khupenia, Omari Lortkipanidze Rethinking the concept of power in contemporary political and international relations.....	13
ლილი ხარჩილავა ამერიკის შეერთებული შტატებისა და ისრაელის სამხედრო-პოლიტიკური თანამშრომლობა	16
Клименко К. В., Ухналь Н. М. Новітні виміри міжнародної безпеки.....	22
Нечипоренко Т. М. Теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки.....	28
Чупіс А. Д. «Гібридний мир»: загроза чи панацея?.....	34
სალომე გოგიშვილი კოოპერატიული უსაფრთხოების თეორიული და პრაქტიკული ასპექტები თანამედროვე საერთაშორისო ურთიერთობებში	40
Іваницька О. П., Чальцева О. М. Особливості безпекової політики іспанії у XX – XXI сторіччях	47
Міщенко І. В. До питання відповідальності за міжнародними договорами про взаємний захист секретної інформації (на прикладі угоди з США)	53
Орленко В. В. Державний контроль як складова міжнародного співробітництва у сфері безпеки.....	57
Рашевська К. Є. Ре-глобалізація як середовище заохочення та розвитку системи прав людини.....	60
Дем'янюк О. Б. М Міжнародне співробітництво з питань енергетичної безпеки.....	65
Фоменко Д. І. Трансформація системи міжнародного співробітництва в умовах російсько-української війни.....	69

Мосієнко О. В., Якобчук В. П. Бренд України у світовому просторі.....	74
გიორგი კლიმაშვილი საერთაშორისო ურთიერთობათა სუბიექტის მნიშვნელობა	78
Козка А. В., Білик А.С. Космічні аномалії як об'єкт наукових досліджень: неоромантика та міжнародний фактор безпеки	81

КРИЗА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Бадер А. В. Російсько-українська війна крізь призму логіки функціонування капіталістичної світ-економіки.....	85
Цокур Є. Г., Чайка І. Ю. Безпекові стратегії в умовах сучасних викликів: новий погляд на симулякр безпеки.....	90
Юлдашев О. Х. Концепція усунення загроз глобальній та регіональній безпеці.....	94
Волторніст О. С. Розмивання традиційних парадигм безпеки: виклики сучасній системі міжнародної безпеки.....	103
Литвин Ю. В., Лакіза В. В. Вплив економічних криз на міжнародну безпеку: шляхи їх подолання.....	107
Швець К. А. Безпека України в міжнародному контексті сучасності.....	111
Фурсай О. В. «Вакцинодемія» як елемент світового гібридного протистояння демократії та автократії.....	115
Прищепа Р. П. REALPOLITIK як практика економічного тиску.....	121

РЕГІОНАЛЬНА БЕЗПЕКА В НОВИХ ГЕОПОЛІТИЧНИХ КОНЦЕПЦІЯХ

Бусленко В. В. Україна в безпековій політиці Республіки Польща ...	125
Стець А. М. Безпека Польщі та України.....	131
Тодоров І. Я., Тодорова Н. Ю. Стійкість та опорність України в контексті євроатлантичної інтеграції	136
ქეთი ჯიჯეიშვილი საქართველო ევროპული ინტეგრაციის გზაზე ..	147

გიორგი ჩხიკვიძეილი საქართველოს ევროპული არჩევანი: ისტორიულ -პოლიტიკური ექსკურსი	141
Gvantsa Abesadze Alignment of Georgia's foreign policy with the European union's foreign and security policy on the path of integration.....	151
Вовченко О. В. Контроль за иноземними субсидіями як фактор регіональної економічної безпеки Європейського Союзу	155
Мацишина І. В. До поняття моралі політичного реалізму в умовах війни.....	159
Райков А. Е. Війна в Нагірному Карабаху як чинник геополітичних змін у регіоні Південного Кавказу	164
Ціватий В. Г. Концепт «кризова дипломатія» і регіональна безпека в умовах трансформації системи міжнародних відносин XXI століття: геополітичний, інформаційно-комунікаційний та інституціональний дискурси	169

ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

Завгородня Ю. В. Політична кіберкультура як елемент кіберстабільності.....	174
Климчук Д. О. Кібербезпека процесу проведення виборів.....	179
Кучмії О. П. Кібербезпека як складова стратегії протидії гібридним викликам і загрозам ЄС	182
Кузьмич В. М. Основні стратегічні напрямки кібербезпеки.....	187
Сімакова С. І. Актуальні питання кібербезпеки в українському суспільстві	191
Суський Г. В. Кібербезпека у проблемному полі гібридної війни.....	195
Гуменюк Н. І., Ангельська В. Ю., Матвійчук М. В., Поляруш В. В. Безпілотні літальні апарати: виклики та перспективи сьогодення... 200	
Крошка Н. В. Діагностування інтернет-залежності у воєнний час в контексті кібербезпеки	205
Кондратенко А. О. Важливість забезпечення безпеки в логістиці	209

КІБЕРЗАХИСТ ТА НАЦІОНАЛЬНА БЕЗПЕКА: УКРАЇНСЬКИЙ ДОСВІД

Гринік А. В., Ярошевська Т. В. Проблемні питання забезпечення кібербезпеки України	213
Дубель М. В. Цифрові віруси як сучасна загроза національній безпеці.....	218
Горошко О. Л. Перспективи навчання кібербезпеки в освітніх інституціях.....	222
Обіход Т. В., Біленчук П. Д. Кібербезпека України: досягнення і перспективи її забезпечення	227
Галюга К. М., Орел О. В. Як захистити свої особисті дані від кібератак	232
Кондратьєва К. А. Місцева електронна демократія України в умовах воєнного стану: питання ефективності	237
Харинович М.-М. С. Протидія загрозам національній безпеці в інформаційному просторі: досвід України	241
Снитко В. В. Кіберзахист та національна безпека: український досвід.....	244
Літинська В. А. Актуальність кібербезпеки у маркетинговій аналітиці.....	247

ЦИФРОВА ДИПЛОМАТІЯ В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

Хорішко Л. С. Особливості співпраці України та НАТО у сфері кібербезпеки	251
Калашлінська М. В. Роль цифрових технологій у підтримці медіації та переговорів в сучасних політичних процесах	255
Сокоринський В. О. Цифровий тоталітаризм як загроза сучасній цифровій дипломатії	258
Рогозіна А. В. Цифрова дипломатія: інформаційний фронт України в умовах війни з росією	262

ФЕЙКИ ТА ДІПФЕЙКИ ЯК ІНСТРУМЕНТИ НЕГАТИВНОГО ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

Вовк С. О. Технологічні аспекти створення дівфейків та їх наслідки для національної безпеки.....	266
Федорова А. І. Фейки російської пропаганди щодо історії України та способи протистояння їм.....	270
Шеломовська О. М. Фейк-ньюз в соціальних мережах: соціологічний аналіз	274
Медведська В. Ю. Діпфейки як загроза розвитку та ефективного функціонування деліберативної демократії в Україні.....	279
Лисичкіна І. О., Лисичкіна О. О. Фейкові новини в сучасному медійному просторі.....	283
Орел О. В. Фейк як інструмент побудови нарративу.....	288
Новік А. К. Російські фейки як фактор ризику національної безпеки України	294

ФАКТЧЕКІНГ ЯК ІНСТРУМЕНТ ПРОТИДІЇ В ГІБРИДНІЙ ВІЙНІ

Суська О. О. «Образ суспільства» та його трансформації в умовах гібридної війни.....	298
Олексунь Н. О., Седляківська К. Г. Загрози та механізми протидії російській пропаганді в умовах війни	304
Супко В. А. Національна та етнічна ідентичність українців в умовах війни (на прикладі Харківщини)	308

ПУБЛІЧНЕ УПРАВЛІННЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА

Примуш М. В. Реформи в обмін на зброю.....	312
Сарибаєва Г. М. Митна безпека в системі національної безпеки України: термінологічний дискурс	315
Абакіна-Пілявська Л. М. До питання динаміки кримінального закону в умовах воєнного стану	320

Гученко К. В. Значення особливості структури особистості суб'єкта злочину дезертирство для національної безпеки	323
Бобось О. Л. Вплив глобальних криз на захист прав споживачів та можливості публічного управління в Україні	329
Ніколаєв К. Д. Екологічні виміри гібридної війни: вплив сучасних загроз на національну та регіональну безпеку	331
Мерзлюк Л. В. Публічно-громадське партнерство та міжнародна співпраця в управлінні регіональною безпекою в умовах сучасних загроз.....	334
Шевченко Р. П. Загрози глобальної та регіональної безпеки та їх вплив на ветеранів війни і членів їх родини	337
Конопля А. І., Лисиця В. В. Цифрова гігієна як засіб формування навичок безпечної роботи в мережі інтернет у дітей дошкільного віку	339
Гуральський Н. Р. Пропозиції державного регулювання засобів масової інформації	343
Ліщук А. О. Публічне управління навчальними закладами на регіональному рівні	347

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ДЕТЕРМІНАНТИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Миросердна І. М. Основні загрози інформаційній безпеці як елементу забезпечення національної безпеки	350
Варнавська І. В. Емоційне вигорання як психологічний феномен ...	355
Бондаренко С. Ю., Вітомський Ю. Л. Психологічні чинники формування національної безпеки держави	359
Лихотоп І. В. Схильність курсантів до нав'ювання.....	364
Бутко О. М., Загоровська М. В., Савченко Л. Л. Інформаційна безпека під час війни.....	369
Куля І. Ф., Беженар К. Д. Інформаційна безпека підприємства	374
Куля І. Ф., Пирлог О. С. Кібергігієна у інформаційному просторі в умовах воєнного стану	381
Куля І. Ф., Спиридонова В. В. Безпека підприємства як основний вид діяльності менеджера підприємства	385

Куля Ірина Федорівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ORCID: 0000-0002-8363-1478

Беженар Карина Дмитрівна

Придунайська філія МАУП, м. Ізмаїл, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

В сучасному світі все частіше постає проблема збільшення інформаційної безпеки підприємств, яка залежить саме від ступеня захищеності інформаційної сфери. Збереження стабільності функціонування та економічного росту, розвиток науково-технічних інновацій залежать від правильної організації інформаційної захищеності підприємств.

Глобальний розвиток інформаційних технологій, модернізована обробка інформації спостерігаються зі зростанням науково-технічного прогресу. Разом з цим і підвищується роль інформаційної безпеки підприємств.

При веденні діяльності кожен підприємець в обов'язковому порядку зіштовхується з необхідністю отримання, зберігання, обробки, перетворення, поширення, передачі та видалення непотрібної або зайвої інформації. Інформація, яка несе користь для підприємства має бути захищеною від зловмисників. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що мають на підприємстві.

Згідно законодавства України інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (Про основні засади розвитку інформаційного суспільства).

Потреба в володінні інформацією призводить до оволодіння інформацією про навколишнє середовище та процеси, що протікають в ньому, тобто інформованості індивіда, соціуму та держави.

Стан та ступінь інформованості впливає на майбутні дії, а також на обґрунтування рішень, які прийматимуться підприємцями.

Загрози інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам підприємств чи підприємців в інформаційній сфері.

Фактори загроз інформаційній безпеці можна класифікувати за видами та ієрархією (рис.1).



Рис. 1. Класифікація факторів загроз інформаційній безпеці

В залежності від виду загроз, інформаційну безпеку можна розглядати як забезпечення стану захищеності (Герасименко, Козак, 2015):

- особистості, суспільства та держави від впливу недостовірної інформації;
- підприємств, організації та інших установ;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод громадянина.

Належний рівень інформаційної безпеки забезпечується сукупністю економічних, організаційних, політичних заходів, спрямованих на попередження, виявлення і нейтралізацію таких обставин, дій і факторів, які можуть завдати шкоди і збитків або перешкодити реалізації інформаційних прав, потреб та інтересів підприємств (Про основні засади розвитку інформаційного суспільства).

Основним і головним завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвочасності або недостовірності інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації.

Забезпечення інформаційної безпеки має бути спрямоване саме на запобігання ризиків, а не на ліквідацію їх наслідків. Тому прийняття запобіжних заходів для забезпечення цілісності, конфіденційності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки. Будь-який витік інформації може призвести до серйозних проблем для підприємства – від значних фінансових збитків до повного припинення існування підприємства (Северина, 2016).

Одним з головних елементів системи інформаційної безпеки підприємств виступають принципи, які мають закладатися в основу її побудови. Основними принципами інформаційної безпеки підприємств є: простота, повний контроль, загальна заборона, відкрита архітектура, розмежування доступу, мінімальні привілеї, стійкість, мінімізація дублювання (рис. 2).

Принцип простоти наголошує на тому, що простота в використанні інформаційної системи здатна забезпечити мінімізацію помилок.

Повний контроль полягає в передбаченні підприємством безперервного контролю за станом інформаційної безпеки та моніторингу всіх подій, що впливають на інформаційну безпеку.

Загальна заборона полягає в забороні доступу до інформаційної системи підприємства, без наданого на це дозволу.

Принцип відкритої архітектури полягає в тому, що безпека має забезпечуватися через неясність. Спроби захистити інформаційну систему від комп'ютерних загроз шляхом заплутування, ускладнення, приховування слабких місць і сторін.

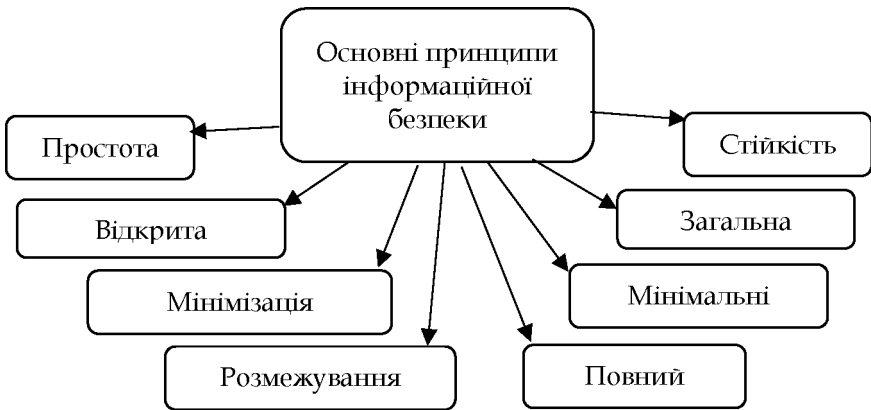


Рис. 2. Основні принципи інформаційної безпеки

Принцип розмежування доступу полягає в тому, що кожному користувачеві надається доступ до інформації, а також її носіїв у відповідності до його повноважень.

Принцип мінімальних привілеїв полягає у виділенні користувачам найменших прав і мінімального доступу до інформаційної системи.

Принцип стійкості інформаційної системи виражається в тому, що потенційні зловмисники мають зустрітися з перешкодами, складними обчислювальними завданнями при потенційній хакерській атаці.

Мінімізація дублювання передбачає мінімізацію ідентичних процедур для декількох споживачів, наприклад, таких як введення паролів.

Побудована за наведеними принципами система інформаційної безпеки має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати структуру системи і основні параметри її функціонування (Рудий, Томаневич, Руда, 2014).

Для підприємств основними цілями досягнення високого рівня інформаційної безпеки є забезпечення її основних складових: цілісності, достовірності, конфіденційності (рис. 3).

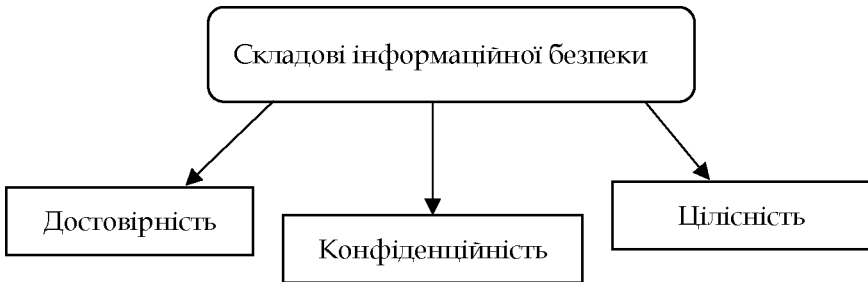


Рис. 3 Складові інформаційної безпеки

Доступність – це можливість за певний період часу одержати необхідну інформаційну послугу.

Цілісність – це актуальність і несуперечність інформації, її захищеність від змін та видалення. В свою чергу цілісність можна розділити на статичну (розуміється як незмінність інформаційних об'єктів) і динамічну (відноситься до коректного виконання певних дій та складних транзакцій).

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана і поширена серед певного кола індивідів.

Успішність функціонування підприємств у динамічному ринковому середовищі значною мірою визначається станом інформаційної безпеки. Рівень економічної безпеки суб'єкта господарювання залежить від того, наскільки ефективною є інформаційна безпека суб'єкта господарювання, що дає змогу уникнути можливих загроз та негативних наслідків впливу конкурентного середовища.

Отже, безпека підприємства – це такий стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективно їхнє використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім та зовнішнім негативним впливам (загрозам) (Архипов, Скиба, 2013).

Відповідно достатній рівень інформаційної безпеки дає змогу підприємству повною мірою використовувати необхідну інформацію для прийняття результативних управлінських рішень, виконання яких обумовить подальшу фінансову стійкість підприємства і буде сприяти його подальшій ефективній роботі (Войнаренко, Рзаєв, Рзаєва, 2014).

Література

Архипов, О., Скиба, А. (2013). Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації*, 15, 4, 350–375.

Василенко, М. (2018). Підвищення стану кібербезпеки інформаційно комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства. *Юридичний вісник*, 3, 17–24.

Герасименко, О. В., Козак, А. В. (2015). *Інформаційна безпека підприємства: поняття та методи її забезпечення*. URL: <http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiy-na-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/>

Іванова, В. *Інформаційна безпека як підсистема в системі економічної безпеки підприємства*. URL: <http://eprints.kname.edu.ua/38599/1/67-71.pdf>.

Войнаренко, М. П., Рзаєв, Г. І., Рзаєва, Т. Г. (2014). *Інформаційна безпека підприємства у динамічному ринковому середовищі*. Хмельницький.

Закон про сновні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки Закон України 2007 (Верховна Рада України). Офіційний сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text>

Рудий, Т., Томаневич, Л., Руда, О. (2014). Засади захисту інформації в інформаційних системах підприємств. *Актуальні проблеми економіки*, 2 (152), 351–387.

Северина, С. (2016). Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки*, 1, 132–154.